00 204

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年　８月３１日

出 願 番 号
Application Number: 特願２０００－２６２９５５

出 願 人
Applicant (s): インターナショナル・ビジネス・マシーンズ・コーポレーション

２００１年　２月２３日

特許庁長官
Commissioner,
Patent Office 及川耕造

CERTIFIED COPY OF
PRIORITY DOCUMENT

出証番号　出証特２００１－３０１１３２０

【書類名】　特許願

【整理番号】　JP9000204

【提出日】　平成12年 8月31日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 19/00

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

【氏名】　丸山　宏

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

【氏名】　工藤　道治

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

【氏名】　田村　健人

【特許出願人】

【識別番号】　390009531

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】　100086243

【弁理士】

【氏名又は名称】　坂口　博

【代理人】

【識別番号】　100091568

【弁理士】

【氏名又は名称】　市位　嘉宏

【代理人】

【識別番号】　100106699

【弁理士】

【氏名又は名称】　渡部　弘道

【復代理人】

【識別番号】　100112520

【弁理士】

【氏名又は名称】　林　茂則

【電話番号】　046-277-0540

【選任した復代理人】

【識別番号】　100110607

【弁理士】

【氏名又は名称】　間山　進也

【選任した復代理人】

【識別番号】　100098121

【弁理士】

【氏名又は名称】　間山　世津子

【手数料の表示】

【予納台帳番号】　091156

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9706050

【包括委任状番号】　9704733

【包括委任状番号】　0004480

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　電子署名システム、電子署名方法、電子署名の仲介方法、電子署名の仲介システム、情報端末および記録媒体

【特許請求の範囲】

【請求項１】　電子文書のサマリテキストを生成するステップと、

前記サマリテキストを署名者の端末の表示画面に表示するステップと、

入力データを一義的に表す値を生成し前記値から入力データを再生成することが困難な関数を用いて前記サマリテキストのダイジェスト値を計算するステップと、

前記ダイジェスト値を含むデータを、前記端末に保有された私有鍵を用いて暗号化し署名値を生成するステップと、

前記署名値を含む署名文書を生成するステップと、

を有する電子署名方法。

【請求項２】　前記電子文書および署名文書はＸＭＬ文書であり、前記ＸＭＬ文書である電子文書のＸＰａｔｈを用いて前記サマリテキストを生成する請求項１記載の電子署名方法。

【請求項３】　前記端末には、変数フィールドを含む署名テンプレートを備え、

前記署名テンプレートの前記変数フィールドに前記ダイジェスト値を組み込むステップと、

前記ダイジェスト値が組み込まれた前記署名テンプレートを前記関数を用いて変換するステップと、

前記変換により生成された値を、前記私有鍵を用いて暗号化し前記署名値を生成するステップと、

を有する請求項１記載の電子署名方法。

【請求項４】　前記署名テンプレートの前記変数フィールドには、さらに前記電子文書のＵＲＩが組み込まれる請求項３記載の電子署名方法。

【請求項５】　前記署名テンプレートは所定のアルゴリズムでカノニカライズされている請求項３記載の電子署名方法。

【請求項６】　前記関数はハッシュ関数である請求項１または３記載の電子署名方法。

【請求項７】　電子文書のサマリテキストを生成する手段と、

前記サマリテキストを署名者の端末の表示画面に表示する手段と、

入力データを一義的に表す値を生成し前記値から入力データを再生成することが困難な関数を用いて前記サマリテキストのダイジェスト値を計算する手段と、

前記ダイジェスト値を含むデータを、前記端末に保有された私有鍵を用いて暗号化する手段と、

前記暗号化によって生成される署名値を含む署名文書を生成する手段と、

を有する電子署名システム。

【請求項８】　前記電子文書および署名文書はＸＭＬ文書であり、前記ＸＭＬ文書である前記電子文書のＸＰａｔｈを用いて前記サマリテキストを生成する手段を含む請求項７記載の電子署名システム。

【請求項９】　前記端末には、変数フィールドを含む署名テンプレートを備え、

前記署名テンプレートの前記変数フィールドに、前記ダイジェスト値を組み込む手段と、

前記ダイジェスト値が組み込まれた前記署名テンプレートを前記関数を用いて変換する手段と、

前記変換により生成された値を前記私有鍵を用いて暗号化する手段と、

を有する請求項７記載の電子署名システム。

【請求項１０】　前記署名テンプレートの前記変数フィールドには、さらに前記電子文書のＵＲＩが組み込まれる請求項９記載の電子署名システム。

【請求項１１】　前記署名テンプレートは所定のアルゴリズムでカノニカライズされている請求項９記載の電子署名システム。

【請求項１２】　前記関数はハッシュ関数である請求項７または９記載の電子署名システム。

【請求項１３】　署名要求者が、電子文書をエージェントに送付するステップと、

前記エージェントが、前記電子文書のサマリテキストを生成し、前記サマリテキストを署名者の端末に送付するステップと、

前記署名者の端末の表示画面に前記サマリテキストを表示するステップと、

前記署名者が前記サマリテキストを確認し、前記端末に保有された私有鍵を用いて、前記サマリテキストまたは前記サマリテキストに対応する文書に電子署名を行うステップと、

前記電子署名により生成された署名値を前記エージェントに送付するステップと、

前記エージェントが、前記署名値を組み込んで、前記電子文書の署名文書を生成するステップと、

前記署名要求者に、前記署名文書を送付するステップと、

を含む電子署名方法。

【請求項１４】　署名要求者が、電子文書をエージェントに送付する手段と、

前記エージェントが、前記電子文書のサマリテキストを生成し、前記サマリテキストを署名者の端末に送付する手段と、

前記署名者の端末の表示画面に前記サマリテキストを表示する手段と、

前記署名者が前記サマリテキストを確認し、前記端末に保有された私有鍵を用いて、前記サマリテキストまたは前記サマリテキストに対応する文書に電子署名を行う手段と、

前記電子署名により生成された署名値を前記エージェントに送付する手段と、

前記エージェントが、前記署名値を組み込んで、前記電子文書の署名文書を生成する手段と、

前記署名要求者に、前記署名文書を送付する手段と、

を含む電子署名システム。

【請求項１５】　署名要求者から署名対象の電子文書を受け取り、前記電子文書のサマリテキストを生成するステップと、

前記サマリテキストを署名者の端末に送付するステップと、

前記署名者の端末から受け取った署名値を組み込んで、前記電子文書に対する

署名文書を生成するステップと、

前記署名文書を前記署名要求者に送付するステップと、

を有する電子署名の仲介方法。

【請求項１６】　前記電子文書および署名文書はＸＭＬ文書であり、前記サマリテキストは、ＸＭＬで記述された前記電子文書のＸＰａｔｈを用いて生成される請求項１５記載の電子署名の仲介方法。

【請求項１７】　署名要求者から署名対象の電子文書を受け取り、前記電子文書のサマリテキストを生成する手段と、

前記サマリテキストを署名者の端末に送付する手段と、

前記署名者の端末から受け取った署名値を組み込んで、前記電子文書に対する署名文書を生成する手段と、

前記署名文書を前記署名要求者に送付する手段と、

を有する電子署名の仲介システム。

【請求項１８】　前記電子文書および署名文書はＸＭＬ文書であり、ＸＭＬで記述された前記電子文書のＸＰａｔｈを用いて前記サマリテキストを生成する手段を有する請求項１７記載の電子署名の仲介システム。

【請求項１９】　電子文書のサマリテキストを受け取る手段と、

前記サマリテキストを画面に表示する表示手段と、

入力データを一義的に表す値を生成し前記値から入力データを再生成することが困難な関数を用いて前記サマリテキストのダイジェスト値を計算する手段と、

私有鍵を記録する記憶手段と、

前記ダイジェスト値を含むデータを、前記私有鍵を用いて暗号化する手段と、

前記暗号化手段により生成された署名値を送信する手段と、

を有する情報端末。

【請求項２０】　前記情報端末には、

変数フィールドを含む署名テンプレートが記録される記憶手段と、

前記署名テンプレートの前記変数フィールドに前記ダイジェスト値および前記電子文書のＵＲＩその他前記電子文書に関する情報を組み込む手段と、

前記ダイジェスト値および情報が組み込まれた前記署名テンプレートを前記関

数を用いて変換する手段と、

前記変換により生成された値を、前記私有鍵を用いて暗号化し前記署名値を生成する手段と、

を有する請求項１９記載の情報端末。

【請求項２１】　前記電子文書はＸＭＬ文書であり、前記署名テンプレートは所定のアルゴリズムでカノニカライズされている請求項２０記載の情報端末。

【請求項２２】　電子文書のサマリテキストを受け取るステップと、

前記サマリテキストを画面に表示するステップと、

入力データを一義的に表す値を生成し前記値から入力データを再生成することが困難な関数を用いて前記サマリテキストのダイジェスト値を計算するステップと、

前記ダイジェスト値を含むデータを、情報端末の記憶領域または前記情報端末に接続できるメモリ手段の記憶領域に記録された私有鍵を用いて暗号化するステップと、

前記暗号化手段により生成された署名値を送信するステップと、

を有する電子署名方法。

【請求項２３】　前記情報端末の記憶領域または前記情報端末に接続できるメモリ手段の記憶領域に記録された署名テンプレートの変数フィールドに、前記ダイジェスト値および前記電子文書のＵＲＩその他前記電子文書に関する情報を組み込むステップと、

前記ダイジェスト値および情報が組み込まれた前記署名テンプレートを前記関数を用いて変換するステップと、

前記変換により生成された値を、前記私有鍵を用いて暗号化し前記署名値を生成するステップと、

をさらに有する請求項２２記載の電子署名方法。

【請求項２４】　前記電子文書はＸＭＬ文書であり、前記署名テンプレートは所定のアルゴリズムでカノニカライズされている請求項２３記載の電子署名方法。

【請求項２５】　公開鍵方式の暗号化に用いる私有鍵の情報が記録され、

コンピュータに、入力データを一義的に表す値を生成し前記値から入力データを再生成することが困難な関数を用いて電子文書のサマリテキストのダイジェスト値を計算する機能と、前記ダイジェスト値を含むデータを前記私有鍵を用いて暗号化する機能と、を実現させるためのプログラムが記録されたコンピュータ読みとり可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、電子署名方法およびシステムに関する。特に署名対象文書がＸＭＬ文書である場合、および、電子署名をＰＤＡ（personal digital assistants）あるいはたとえばｉモード通信対応の携帯電話等で行う場合に適用して有効な技術に関する。

【０００２】

【従来の技術】

ネットワーク技術の発達により、情報の伝達媒体は紙から電子データそれ自体に移行しつつある。従来紙媒体に記録されている内容（情報）の個人的な確認行為として署名あるいは捺印がある。しかし、電子データは容易に複製でき、また、通信途中での改ざんの機会も増えることからセキュリティの確保できる電子署名技術が欠かせない。

【０００３】

データ暗号化の方式として公開鍵暗号（非対称暗号と称される場合もある）と共通鍵暗号（対称暗号と称される場合もある）が良く知られている。共通鍵暗号はセキュアな通信を行う送り手と受け手の間で共通の鍵（共通鍵：秘密鍵と称される場合もあるが本明細書では後述の私有鍵との混乱をさけるために共通鍵の用語を用いる。）を保持し、送り手は共通鍵で暗号化した情報を送出し、受け手は共通鍵を用いてこれを解読する。この方式の前提として共通鍵情報を秘密裏に共有する必要がある。鍵情報に関する秘密が解除されたときには通信のセキュリティは保証されない。

【０００４】

一方、公開鍵暗号方式は、公開鍵および私有鍵（秘密鍵と称される場合もある）の鍵ペアを有し、いずれかの鍵で暗号化した情報は他方の鍵を用いなければ実質的に解読できない方式である。予め入手した通信相手の公開鍵で情報を暗号化し、この暗号化情報を通信相手である他人に送付する。通信相手は自己の私有鍵を用いてこれを解読する。この方式のメリットは公開鍵を公開しても通信のセキュリティは阻害されず、通信の前提として秘密の鍵情報を共有する必要が無い点である。電子署名はこのような公開鍵暗号を用いて行うことができる。つまり、署名者本人しか知り得ない私有鍵を用いて署名対象文書を暗号化し、この暗号情報を受け取った者は、その私有鍵に対応する公開鍵を入手してこれを解読し、署名文書の内容を確認できる。この場合、公開されている公開鍵が署名者本人のものであると信ずるに足る根拠が必要であるが、この本人確認には認証機関（ＣＡ：certification authority）の認証サービスを利用できる。逆に本人にとっては私有鍵の保護は重要である。仮に私有鍵が漏洩した場合にはその私有鍵を用いて他人が鍵の所有者になりすますことができる。よって、電子署名において（暗号通信あるいは鍵配布においても）私有鍵の保護は絶対的な条件である。

【０００５】

ところで、近年の電子取引（e-business）においては、交換されるデータの形式としてＸＭＬ文書が採用されつつある。ＸＭＬは、いわば自己定義型の構造化文書であるため、ますます複雑化する交換データを効果的に取り扱うことが可能になる。Ｂ２Ｂ（business to business）取引はもとよりＢ２Ｃ（business to consumer）取引においてもＸＭＬが標準的に用いられる可能性が高い。

【０００６】

このような背景からＷ３Ｃ（www consortium）において、ＸＭＬのためのディジタル署名仕様、ＸＭＬＤＳＩＧが策定されつつある。（たとえばhttp://www.w3.org/Signature/を参照されたい。）ＸＭＬ電子署名の技術は、データ改ざんの防止およびトランザクションの証拠性確保の切り札として期待されている。

【０００７】

【発明が解決しようとする課題】

前記した通り、私有鍵の保護は本人であることを証明するため、あるいは他人

のなりすましを防止するために重要である。このため、私有鍵をパーソナルコンピュータのハードディスク等に記録して保管するのは安全ではない。よって、スマートカード等、常に本人が携帯できるセキュリティ・トークンに記憶することが好ましい。

【０００８】

しかし、スマートカード自体には、表示機能が存在しない。このため、カードリーダを有するパソコン等の画面等を見て署名対象の文書内容を確認することになる。たとえば商店で商品を購入して電子決済する場合の決済確認文書に署名をする場合には、商店のパソコン画面あるいはＰＯＳ端末の画面等を用いて文書内容を確認することになる。このとき、表示された文書が真に信頼できるかについては疑問が残る。上記例の場合、仮に決済機関から端末に送付された文書内容が端末で改ざんされて表示されていた場合には、利用者はこの改ざんの事実を感知することはできず、自己の認識とは異なる文書に署名を施す危険性を排除できない。

【０００９】

このような不安を払拭するには、十分に信頼できる端末、たとえば自己所有のＰＤＡやｉモード携帯電話等を用いて署名対象文書を確認することが望ましい。

【００１０】

ところが、携帯端末に電子署名機能を実装するには以下の問題がある。特に今後発展すると期待できるＸＭＬ電子署名を携帯端末で実現しようとすると問題が顕著になる。

【００１１】

すなわち、携帯端末では、その表示画面が小さいため署名対象文書の全文を表示することが困難である。特にＸＭＬ文書の場合、タグ情報あるいはその他ＤＳＩＧの仕様に基づく情報も含めて表示するには携帯端末の表示画面面積は十分でない。

【００１２】

また、携帯端末の計算資源は一般に制限されている。このため署名に必要な計算を携帯端末に行わせるには負荷が大きい。特にＸＭＬ電子署名の場合には、Ｘ

ＭＬプロセッサあるいはＸＰａｔｈプロセッサ等を要求するため、計算資源の限られている携帯端末でそれを実現するにはコストが大きくなる。

【００１３】

本発明の目的は、携帯端末のように計算資源の限られた情報処理端末を用いてＸＭＬ電子署名を行う技術を提供することにある。

【００１４】

また、本発明の目的は、より安全性の高い電子署名方法、システムあるいは電子署名用端末を提供することにある。

【００１５】

【課題を解決するための手段】

本願の発明の概略を説明すれば、以下の通りである。すなわち、本発明の電子署名方法では、たとえばＸＭＬ文書等の署名対象文書をエージェントが署名者に代わって受け取り、エージェントによって署名対象文書のサマリテキストが生成される。サマリテキストは署名者に送付され、署名者は自己の所有する情報端末でこのサマリテキストを表示し、その内容を確認する。サマリテキストの内容を確認後、署名者はサマリテキストに対して、自己の端末に記録された私有鍵を用いて暗号化し署名をする。署名値（暗号化データ）はエージェントに送られ、エージェントは署名値を含んだ署名対象文書に対する署名文書を生成し、署名要求者にこれを送付する。書名要求者は署名文書を受け取り、署名者の公開鍵を用いて解読し署名内容を確認する。

【００１６】

このような署名方法によれば、ユーザ（署名者）は、自己の端末で表示できる形式（たとえばテキスト形式）に変換されたサマリテキストを表示して文書の内容を確認できる。また、サマリテキストの暗号化にはＸＭＬプロセッサ等の計算負荷がかからず、携帯端末等の計算資源が限られた機器でも十分に行うことができる。自己所有の端末を用いるのでその表示は十分信頼するに足り、また、私有鍵は自己所有の端末に記録されるので、私有鍵の保全も十分に行うことができる。これにより安全な電子署名方法を提供できる。なお、このような署名方法によれば、署名者はサマリテキストの内容について責任を負い、署名対象文書にあっ

てサマリテキストにはない内容についてはエージェントとユーザ（署名者）との間で取り決める範囲で責任を分担することになる。

【００１７】

サマリテキストの生成には、たとえばＸＭＬ文書のＸＰａｔｈを利用しＸＭＬ要素の内容（文字列）を抜き出して生成できる。ＸＭＬ電子署名はこのようなＸＰａｔｈの適用を許しており、このようにして作られたＸＭＬ電子署名文書は、ＸＭＬ電子署名の標準に準拠したものにすることができる。

【００１８】

サマリテキストへの署名は、サマリテキストを、入力データを一義的に表す値を生成しその値から入力データを再生成することが困難な関数、たとえば一方向ハッシュ関数を用いてハッシュ値（ダイジェスト値）を生成し、このダイジェスト値を含む文書を端末内の私有鍵で暗号化することができる。また、端末には署名テンプレートを備えることができる。署名テンプレートには変数フィールドを有し、サマリテキストのハッシュ値（ダイジェスト値）を変数フィールドに組み込む。署名テンプレートの全体をハッシュ変換しさらに私有鍵で暗号化して署名値とすることができる。署名テンプレートには署名対象文書（電子文書）のＵＲＩを組み込むこともできる。

【００１９】

このような署名テンプレートを用いた署名により、端末にＸＭＬプロセッサ、ＸＰａｔｈプロセッサを実装することなく、ＸＭＬディジタル署名の仕様に準拠した署名を行える。すなわち、署名テンプレートを予めＸＭＬディジタル署名の仕様に準拠した形態で用意し端末に記録しておく。そしてＸＭＬで記述される署名文書に必要な署名値を端末側で生成する。この署名値はエージェントで生成されるＸＭＬ署名文書に組み込まれる。つまり、端末側ではサマリテキストのハッシュ値の生成、ハッシュ値のテンプレートへの組み込み（およびＵＲＩの組み込み）、テンプレートのハッシュ値の生成、およびその暗号化を行えばよく、ＸＭＬプロセッサ等の機能は必要ではない。

【００２０】

なお、署名テンプレートは所定のアルゴリズムでカノニカライズ（規範化）で

きる。これにより空白あるいは記号等の文書のゆらぎを統一することができる。

【００２１】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて詳細に説明する。ただし、本発明は多くの異なる態様で実施することが可能であり、本実施の形態の記載内容に限定して解釈すべきではない。なお、実施の形態の全体を通して同じ要素には同じ番号を付するものとする。

【００２２】

以下の実施の形態では、主に方法またはシステムについて説明するが、当業者であれば明らかなとおり、本発明は方法、システムの他、コンピュータで使用可能なプログラムが記録された媒体としても実施できる。したがって、本発明は、ハードウェアとしての実施形態、ソフトウェアとしての実施形態またはソフトウェアとハードウェアとの組合せの実施形態をとることができる。プログラムが記録された媒体としては、ハードディスク、ＣＤ－ＲＯＭ、光記憶装置または磁気記憶装置を含む任意のコンピュータ可読媒体を例示できる。

【００２３】

また以下の実施の形態では、一般的なコンピュータシステムを用いることができる。実施の形態で用いるコンピュータシステムには、中央演算処理装置（ＣＰＵ）、主記憶装置（メインメモリ：ＲＡＭ）、不揮発性記憶装置（ＲＯＭ）等を有し、バスで相互に接続される。バスには、その他コプロセッサ、画像アクセラレータ、キャッシュメモリ、入出力制御装置（Ｉ／Ｏ）等が接続されてもよい。バスには、適当なインターフェイスを介して外部記憶装置、データ入力デバイス、表示デバイス、通信制御装置等が接続される。その他、一般的にコンピュータシステムに備えられるハードウェア資源を備えることが可能なことは言うまでもない。外部記憶装置は代表的にはハードディスク装置が例示できるが、これに限られず、光磁気記憶装置、光記憶装置、フラッシュメモリ等半導体記憶装置も含まれる。データ入力デバイスには、キーボード等の入力装置、マウス等ポインティングデバイスを備えることができる。データ入力デバイスにはスキャナ等の画像読み取り装置、音声入力装置も含む。表示装置としては、ＣＲＴ、液晶表示装

置、プラズマ表示装置が例示できる。また、コンピュータシステムには、パーソナルコンピュータ、ワークステーション、メインフレームコンピュータ等各種のコンピュータが含まれる。

【００２４】

図１は、本発明の電子署名システムの一例を示したブロック図である。本実施の形態の電子署名システムは、インターネット１に接続された署名要求者システム２、エージェントシステム３、ユーザ（署名者）端末４を有する。

【００２５】

本実施の形態ではインターネット１を例示するが、これに限られず、署名要求者システム２、エージェントシステム３およびユーザ端末４は有線あるいは無線の専用回線回線を通じて接続されてもよい。また、インターネット１に限らず、特定のユーザのみがアクセスできるプライベートなイントラネットでも良い。何らかの通信手段を用いて前記各システム、端末が相互に接続される限り、本発明に含まれる。

【００２６】

署名要求者システム２は、署名を要求する者のシステムであり、署名対象文書を発行する。署名対象文書は後に詳しく説明するようにたとえばＸＭＬ文書である。署名要求者システム２には、前記の通り一般的なコンピュータ・システムを用いることができる。署名要求者システム２はたとえば電子商取引サイト（ＥＣサイト）を例示できる。後に説明するように、たとえば電子取引における物品（後の例では本）の販売において、注文文書にサイン（署名）を求める場合に本発明が利用できる。ＥＣサイトとしては、注文者（ユーザ）が後に否認できない状態の注文書（つまり注文者によるサインのある注文書）を取得してから物品を発送することが商取引の安全上好ましい。この場合の注文書は電子文書たとえばＸＭＬ文書でありそのサインは電子署名たとえばＸＭＬ電子署名になる。本発明は電子商取引の安全性を高めて健全な取引秩序の形成に寄与できる。なお、本実施の形態の電子署名システムは、いうまでもなくＥＣサイト用途には限られない。つまりサインした者に後に否認させないための証拠として活用できる限り、本発明の署名システムを利用できる。たとえばインターネットあるいはイントラネッ

ト上で交換される社内文書に承認を与える場合の署名行為に本システムを活用できる。つまり、署名要求者にはＥＣサイトのほかに社内の承認権限を有する者、その他契約当事者等あらゆるサイン要求者を含めることができる。

【００２７】

エージェントシステム３は、エージェントのシステムである。エージェントは署名要求者と署名者との間を仲介する者であり、両者にとって信頼できる第３者である。エージェントシステム３は署名対象文書からサマリテキストを生成する。そして後に説明するように端末４で生成された署名値を組み込んで署名要求文書に対する署名文書を生成する。つまり、エージェントシステム３は署名要求文書のうち、サマリテキストの部分についてのみユーザ（署名者）に署名を求め、この署名値に基づいて署名要求者の要求する署名文書を生成する。

【００２８】

サマリテキストは署名対象文書の中心的な内容をユーザの端末４でも表示できるように変換した文書であり、たとえばテキスト文書を例示できる。このようにエージェントによってサマリテキストに変換されるため、端末４ではこのサマリテキストを表示すれば足り、ＸＭＬ文書の全体を表示する必要がない。端末４がＰＤＡ、携帯電話のように表示画面の小さなものであっても文書の表示が容易に行える。また、ユーザ端末４ではサマリテキストについての暗号化を行い、基本的にはＸＭＬ文書を取り扱う必要がない。すなわち、エージェントシステム３は、契約（約束）の実体的な部分についてはサマリテキストとしてユーザに署名を求め、ＸＭＬに適合させるための形式的な部分についての代行を行う。このためユーザ端末４ではＸＭＬプロセッサ等を実装する必要がなく、計算負荷を低減してコストを低くすることができる。

【００２９】

ユーザ端末４は、ユーザの所持する情報端末である。たとえばＰＤＡ、ｉモード携帯電話を例示できる。ユーザ端末４には小画面の表示画面を有し、また、ユーザの私有鍵が記録される。ユーザは私有鍵を自己の携帯する端末に記録するので私有鍵の保護を十分に図ることができる。また、電子署名をこの端末４を用いて行う場合には、自己の所有する画面を用いてサマリテキストを表示できるので

その表示を信頼することができる。

【００３０】

またユーザ端末４には署名テンプレートが記録されている。署名テンプレートの機能については後述する。

【００３１】

なお、ユーザ端末４が携帯電話である場合には、キャリア（電話事業者）の交換機５を介してインターネット１に接続される。ユーザ端末４がＰＤＡである場合にはインターネットサービスプロバイダ（ＩＳＰ５）を介してインターネット１に接続される。但し、これら携帯端末は直接ＩＰアドレスを取得してインターネット１に接続されても良いことはもとよりである。

【００３２】

また、本実施の形態ではユーザ端末４としてＰＤＡ、携帯電話等の携帯端末を例示するが、これに限られず、一般的なコンピュータシステムであっても良いことは勿論である。但し、表示画面が小さく計算資源に制限のある携帯端末の場合に本発明を適用して効果が顕著なことはいうまでもない。

【００３３】

また、本実施の形態ではエージェント３を独立したシステムとして説明しているが、署名要求者システム２がエージェント３の機能を有しても良く、またエージェント３の機能をキャリア（電話事業者）５あるいはＩＳＰ５が有してもよい。さらにアプリケーションサービスプロバイダ（ＡＳＰ）がそのサービスの一部としてエージェント３の機能を有しても良い。

【００３４】

図２は、本実施の形態の署名方法の一例を示したフローチャートである。また図３は図２の署名部分の一例を詳細に示したフローチャートである。図２において左側に署名要求者側の処理を、中央部にエージェントの処理を、右側に署名者側の処理を示す。

【００３５】

まず、署名要求者システム２において署名対象文書を生成する（ステップＳ１０）。図４は署名対象文書の一例を示したリスト図である。図４に示すように、

署名対象文書はＸＭＬで記述される。ＸＭＬ文書で情報を交換することにより複雑な取引を効果的に行うことができる。なお、図４のリスト図において、左側に示した番号は行番号である。以下、図５～図７のリスト図について同じである。

【００３６】

図４に示すＸＭＬ文書は本の注文書の一例を示したものである。<Invoice>タグで文書が送り状であることを記述し（行番号１～２５）、<bookorder>タグで囲まれた部分で本の注文内容を記述する（行番号３～１０）。注文内容にはタイトル、ＩＳＢＮコード、数量、価格が記述され、各々<title>タグ、<ISBN>タグ、<quantity>タグ、<price>タグで囲まれた内容が記述される。また、<payment>タグで囲まれた部分には支払いに関する情報が記述される（行番号１１～２４）。支払い先、支払い元、価格、支払期日、支払い方法が各々<payTo>、<billedTo>、<amount>、<dueDate>、<paymentMethod>の各タグで囲んだ内容で記述されている。また、支払い方法がカードであること、各種カード情報が記述されている（行番号１６～２３）。なお、このような送り状（ＸＭＬ文書）が一例であることはいうまでもない。

【００３７】

署名要求者（ここでは本の販売者）がこのような送り状を作成し、この送り状に確認のサイン（署名）を要求する例を以下に説明する。作成された署名対象文書は署名要求者システム２からエージェントシステム３に送付され、エージェントシステム３では署名対象文書を受け取ってこれを記録する（ステップＳ１１）。

【００３８】

次にエージェントシステム３では、署名対象文書からサマリテキストを生成する（ステップＳ１２）。図５は生成されたサマリテキストの例を示すリスト図である。サマリテキストの生成にはＸＰａｔｈを用いる。つまりエージェントシステム３にはＸＰａｔｈプロセッサが実装され、署名対象文書（図４の送り状）に基づいて自動的に生成される。図５に示すように、サマリテキストは注文と支払いの主要部分のみを抽出したテキスト形式の文書である。

【００３９】

次に、エージェントシステム３からユーザ端末４にサマリテキストが送付され、ユーザ端末４ではこれを受け取り表示する（ステップＳ１３）。前記の通りサマリテキストは確認に必要な重要部分のみを抜き出したプレインテキストである。このため、小画面のユーザ端末４でも十分に表示できる。

【００４０】

ユーザはこの信頼できる表示画面に表示された内容（サマリテキストの内容）を確認し（ステップＳ１４）、その内容に承諾する場合には署名を行う（ステップＳ１５）。

【００４１】

図３は、署名操作の一例を示したフローチャートである。署名操作においては、まず、確認したサマリテキストのダイジェスト値を計算する（ステップＳ２０）。ダイジェスト値の計算にはたとえばハッシュ関数を用いる。但し、ハッシュ関数に限る必要はなく、入力に対して一義的な値を出力し、その出力値から容易に入力に逆変換できないような関数であればこれを用いることができる。

【００４２】

次に、ダイジェスト値および署名対象ＵＲＩを署名テンプレートに導入する（ステップＳ２１）。図６は署名テンプレートの一例を示したリスト図である。署名テンプレートは、署名対象文書（ここでは図４の注文書）に適合するように予め生成されており、ＸＭＬディジタル署名の仕様に適合するものである。

【００４３】

また、署名テンプレートには変数フィールドを有する（行番号７、２４）。ここでは署名対象のＵＲＩとサマリテキストのダイジェスト値が各々変数フィールドに割当てられる。サマリテキストのダイジェスト値（ハッシュ値）と署名対象文書のＵＲＩは、この変数フィールドに組み込まれる。

【００４４】

また、署名テンプレートは所定のアルゴリズムでカノニカライズされている。このため、文字コード、空白、記号等のゆらぎをなくすことができる。これらわずかなゆらぎは文書の内容に影響しないものであってもハッシュ値の相違は顕著であり、署名内容を検証する時の障害になる。カノニカライズすることによりこ

のような障害の発生を防止できる。

【００４５】

次に、サマリテキストのダイジェスト値および署名対象ＵＲＩが組み込まれた署名テンプレートの全体についてダイジェスト値を計算する（ステップＳ２２）。ダイジェスト値の計算には、前記同様にハッシュ関数を用いることができる。

【００４６】

その後、署名テンプレート全体のダイジェスト値について私有鍵で暗号化を施す（ステップＳ２３）。これら一連の操作が署名操作であり、暗号化の結果生成された値が署名値になる。

【００４７】

なお、これらユーザ端末４における操作は、サマリテキストおよびテンプレートに対するハッシュ値の計算と私有鍵による暗号化計算のみである。テンプレートもここでは所定のカノニカライズ方法で指定された文字コード（ユニコード）で記述されたテキスト文書であり、ＸＭＬ文書に対するＸＭＬプロセッサ等の操作ではない。つまり、計算資源の限定された機器においても十分に実行できる負荷の小さな操作である。よって、ユーザ端末としてＰＤＡ等の計算資源の限られた情報端末を用いる場合に本発明の効果が大きい。

【００４８】

また、前記ユーザ端末における操作は、ＸＭＬディジタル署名の仕様に適合した形式で行わなければならない。この仕様はカノニカライズのメソッドや署名メソッド、サマリテキストへのトランスフォームの仕方、ダイジェストメソッド等が指定できる。そしてこれら指定は署名文書および署名テンプレートに記述される。たとえば、図６の署名テンプレートにおいては、カノニカライズメソッドは行番号２～３に記述されており、このようなメソッドに従ったカノニカライズが行われている必要がある。また、署名メソッドは行番号４，５に記述され、ここではＤＳＡが指定されている。よって、ステップＳ２３における暗号化はＤＳＡで行われる必要がある。同様に署名対象文書からサマリテキストへの変換はトランスフォーム（行番号９～１９）に従い、ダイジェスト値の計算（行番号２０、２１）はＳＨＡ１による必要がある。なお、署名テンプレートはカノニカライズ

されているのでユニコード（ＵＴＦ－８）で記述されている。

【００４９】

以上のようにして生成された署名値はエージェントシステム３に送付され、エージェントシステム３はこれを受け取って署名文書を生成する（ステップＳ１６）。図７は生成された署名文書の一例を示すリスト図である。署名文書は前記署名テンプレートに適合するように、つまり署名テンプレートに記述されている署名情報（<SignedInfo>）と同じ情報が記述されている。そして、署名対象ＵＲＩに「"http://www.myagent.com/myorder/2000/0321.xml"」（この値は署名テンプレートに組み込んだ値と同じである。）を組み込み、ユーザ端末４から受け取ったダイジェスト値（行番号１９）および署名値（行番号２４）を組み込む。署名者の公開鍵情報（行番号２６～４４）を加えて署名文書とする。

【００５０】

そして、エージェントシステム３はこの署名文書を署名要求者システム２に送信し、署名要求者システム２では署名文書を受け取って内容を確認する（ステップ１７）。署名要求者は、署名文書の公開鍵情報（行番号２６～４４）を用いて署名値（行番号２４）を解読し、一方、署名情報（行番号３～２２）を用いて文書のサマリテキストの生成、そのダイジェスト値の生成等を行い、暗号化前のハッシュ値を計算できる。解読したハッシュ値と計算されたハッシュ値を比較して一致すれば署名の正当性が確認できる。

【００５１】

このような署名方法および署名システムによって、携帯端末等の計算資源が限られ、また、表示画面面積の小さな情報端末を用いてＸＭＬディジタル署名（ＸＭＬＤＳＩＧ）を行うことが可能になる。本実施の形態のシステムおよび方法では、私有鍵が携帯可能な情報端末に記録されるため一種のセキュリティ・トークンとして機能させることができ、私有鍵の安全性を高めることができる。さらに、署名者は信頼できる表示画面を用いてサマリテキストの内容を確認できるので取引の信頼性を高めることができる。

【００５２】

なお、署名者は、サマリテキストについてのみ署名を行うので、署名した範囲

内についてのみ責任が問われる。逆にＸＭＬ文書に何が含まれていようとも自己の責任は署名したサマリテキストの範囲内に限定できる。一方、エージェントの責任範囲についてはそのポリシーにより各種レベルの保証サービスを行うことが可能である。

【００５３】

たとえば「無保証ポリシー」がある。このポリシーにおいては、エージェントは署名外内容については一切の責任を持たない。

【００５４】

また「事後改ざん防止ポリシー」がある。このポリシーにおいては、署名外内容が悪意のある第３者によって、事後に書き換えられることを防止する。エージェントは署名対象ＸＭＬ文書を自ら署名し保管する。あるいは、外部の公証サービスに依頼してもよい。

【００５５】

また、「事前セッション記録ポリシー」がある。このポリシーにおいては、エージェントはこの署名にいたる一連のセッションの存在について保証する。このためには、購入の際にいろいろなオプションを選んだり、条件をつけたりする一連のインタラクションが、エージェント経由で行われなければならない。エージェントはこれらの事前セッションの記録とともに署名対象文書を自らが署名し、保管する。悪意のあるユーザーがいたとしても、ユーザーの端末にどのような情報を送ったかの証拠が残るので、電子商取引サイト側は署名外内容について、ある程度の保証が得られる。一方、ユーザー側も「何を見ていないか」の保証が得られるので、知らないことは知らないと言い張ることができる。

【００５６】

また、「署名対象文書内容チェックポリシー」がある。このポリシーでは、署名外内容について、ユーザーに不利な条項が無いことを、ユーザーのプロファイルに基づいてエージェントがチェックする。このチェックの内容については、事前にユーザーとエージェントが取り交わした契約に基づく。もし、不正直なエージェントについて不安があれば、前記した事後改ざん防止ポリシーと外部公証サービスを組み合わせることによって、不正なチェックを事後に発見することがで

きる。

【００５７】

さらに、これらのポリシーを組み合わせることによって、エージェントは柔軟なサービスを提供することができる。

【００５８】

以上、本発明者によってなされた発明を発明の実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能である。たとえば、前記実施の形態では、私有鍵および署名テンプレートがユーザ端末４に記録されている例を示したが、たとえば、スマートカード等の着脱可能な記録媒体に、私有鍵、署名テンプレートが記録されており、記録媒体が端末に装着されて、これら情報が読み出されるように構成してもよい。さらに、署名計算用のプログラムも含めて、着脱可能な記録媒体に記録し、この記録媒体が、端末４に装着されて、前記したような署名が行なえるように構成してもよい。

【００５９】

【発明の効果】

本願で開示される発明のうち、代表的なものによって得られる効果は、以下の通りである。すなわち携帯端末のように計算資源の限られた情報処理端末を用いてＸＭＬ電子署名を行うことができる。また、より安全性の高い電子署名方法、システムあるいは電子署名用端末を提供できる。

【図面の簡単な説明】

【符号の説明】

【図１】

本発明の電子署名システムの一例を示したブロック図である。

【図２】

本発明の一実施の形態である署名方法の一例を示したフローチャートである。

【図３】

署名操作の一例を示したフローチャートである。

【図４】

署名対象文書の一例を示したリスト図である。

【図５】

生成されたサマリテキストの例を示すリスト図である。

【図６】

署名テンプレートの一例を示したリスト図である。

【図７】

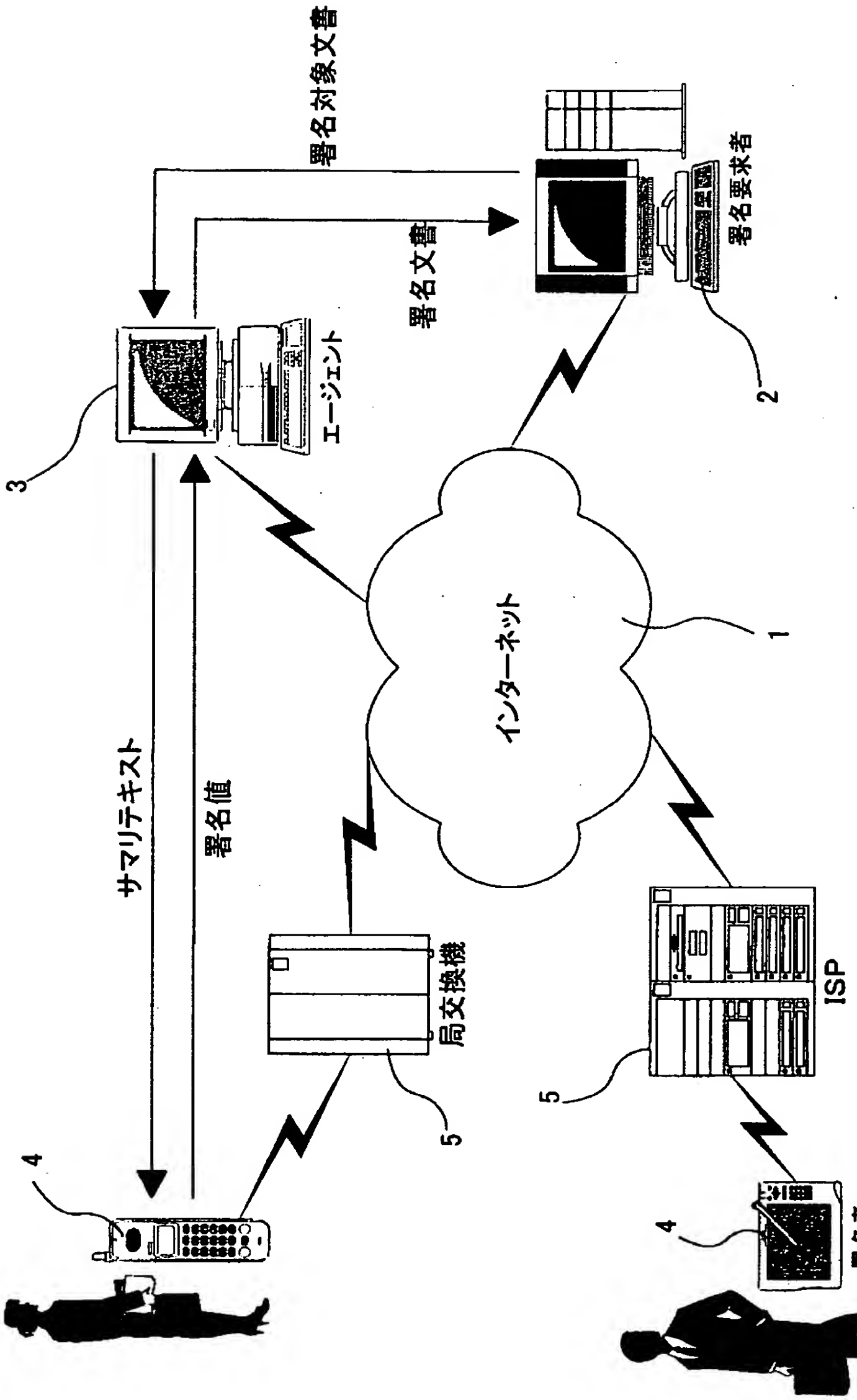
生成された署名文書の一例を示すリスト図である。

【符号の説明】

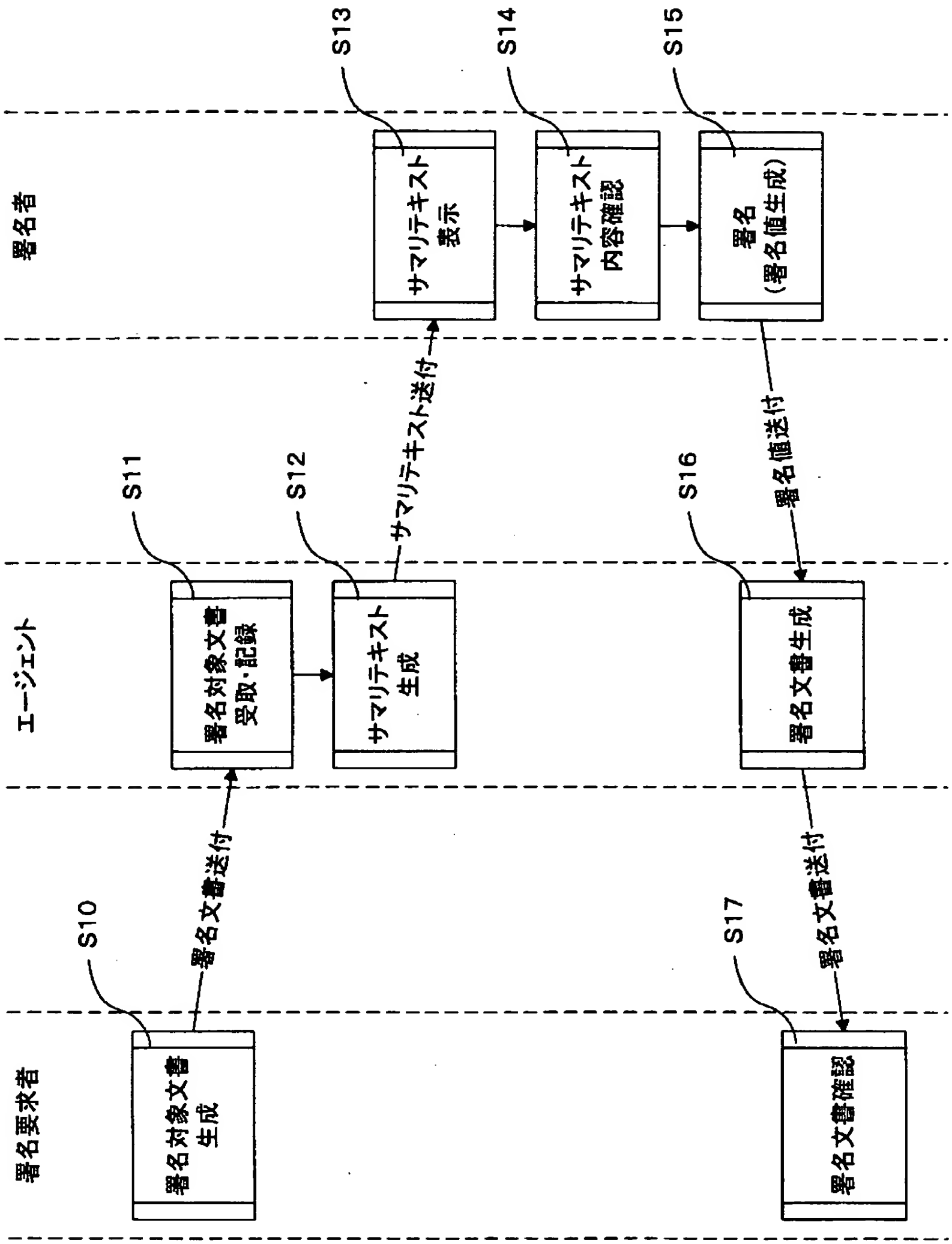
１…インターネット、２…署名要求者システム、３…エージェントシステム（エージェント）、４…ユーザ端末、５…交換機・ＩＳＰ。

【書類名】　　図面

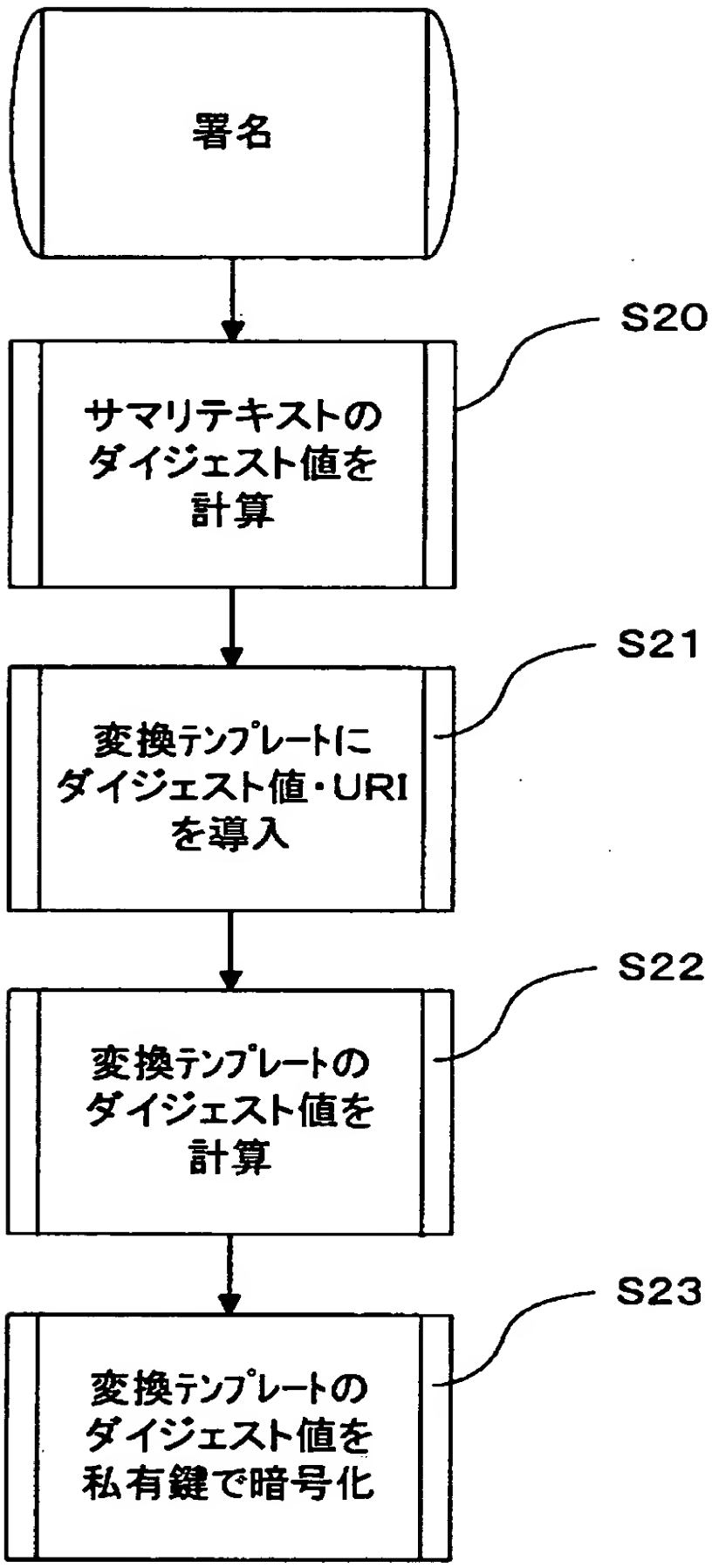
【図１】


署名対象文書
署名文書
署名要求者
エージェント
3
2
インターネット
1
サマリテキスト
署名値
局交換機
5
ISP
4
署名者

【図２】


署名者
S13
サマリテキスト
表示
S14
サマリテキスト
内容確認
S15
署名
(署名値生成)
エージェント
S11
署名対象文書
受取・記録
S12
サマリテキスト
生成
S16
署名文書生成
署名要求者
S10
署名対象文書
生成
S17
署名文書確認

【図３】


署名
S20
サマリテキストの
ダイジェスト値を
計算
S21
変換テンプレートに
ダイジェスト値・URI
を導入
S22
変換テンプレートの
ダイジェスト値を
計算
S23
変換テンプレートの
ダイジェスト値を
私有鍵で暗号化

【図４】

```
<?xml version="1.0" encoding="UTF-8"?>
<Invoice>
  <bookorder>
    <item>
      <title>XML and Java</title>
      <ISBN>0201485435</ISBN>
      <quantity>1</quantity>
      <price>39.95</price>
    </item>
  </bookorder>
  <payment>
    <payTo>AAAAA.com, Inc.</payTo>
    <billedTo>Hiroshi Maruyama</billedTo>
    <amount unit="USD">39.95</amount>
    <dueDate>Apr., 3, 2000</dueDate>
    <paymentMethod>
      <creditCard>
        <cardType>MasterCard</cardType>
        <cardHolderName>Hiroshi Maruyama</cardHolderName>
        <expirationDate>04/2001</expirationDate>
        <cardNumber>5283 8304 6232 0010</cardNumber>
      </creditCard>
    </paymentMethod>
  </payment>
</Invoice>
```

【図５】

```
I, Hiroshi Maruyama, will pay 39.95 USD
to AAAAA.com, Inc. by Apr., 3, 2000
for the purchase of 1 QTY of book titled
XML and Java.
```

【図６】

```
<n1:SignedInfo xmlns:n1="http://www.w3.org/2000/01/xmldsig/">
 <n1:CanonicalizationMethod xmlns:n1="http://www.w3.org/2000/01/xmldsig/"
   Algorithm="http://www.w3.org/TR/1999/WD-xml-c14n-19991115"></n1:CanonicalizationMethod>
 <n1:SignatureMethod xmlns:n1="http://www.w3.org/2000/01/xmldsig/"
   Algorithm="http://www.w3.org/2000/01/xmldsig/dsa"></n1:SignatureMethod>
 <n1:Reference xmlns:n1="http://www.w3.org/2000/01/xmldsig/"
   URI="%署名対象URI%">
  <n1:Transforms xmlns:n1="http://www.w3.org/2000/01/xmldsig/">
   <n1:Transform xmlns:n1="http://www.w3.org/2000/01/xmldsig/"
     Algorithm="http://www.w3.org/TR/1999/PR-xpath-19991008">
    concat("I, ", /Invoice/payment/billedTo, ", will pay ", /Invoice/payment/amount, " ",
          /Invoice/payment/amount/@unit, " to ", /Invoice/payment/payTo, " by ",
          /Invoice/payment/dueDate, " for the purchase of ",
          /Invoice/bookorder/item/quantity, " QTY of book titled ",
          /Invoice/bookorder/item/title, ".")
   </n1:Transform>
   <n1:Transform xmlns:n1="http://www.w3.org/2000/01/xmldsig/"
     Algorithm="http://www.w3.org/TR/1999/WD-xml-c14n-19991115"></n1:Transform>
  </n1:Transforms>
   <n1:DigestMethod xmlns:n1="http://www.w3.org/2000/01/xmldsig/"
     Algorithm="http://www.w3.org/2000/01/xmldsig/sha1"></n1:DigestMethod>
   <n1:DigestValue xmlns:n1="http://www.w3.org/2000/01/xmldsig/"
     Encoding="http://www.w3.org/2000/01/xmldsig/base64">
     %サマリテキストのダイジェスト値%
   </n1:DigestValue>
  </n1:Reference>
</n1:SignedInfo>
```

【図７】

```
<?xml version="1.0" encoding="UTF-8"?>
<Signature xmlns="http://www.w3.org/2000/01/xmldsig/">
 <SignedInfo>
  <CanonicalizationMethod Algorithm="http://www.w3.org/TR/1999/WD-xml-c14n-19991115"/>
  <SignatureMethod Algorithm="http://www.w3.org/2000/01/xmldsig/dsa"/>
  <Reference URI="http://www.myagent.com/myorder/2000/0321.xml">
   <Transforms>
       <Transform Algorithm="http://www.w3.org/TR/1999/PR-xpath-19991008">
    concat("I, ", /Invoice/payment/billedTo, " will pay ", /Invoice/payment/amount, " ",
         /Invoice/payment/amount/@unit, " to ", /Invoice/payment/payTo, " by ",
         /Invoice/payment/dueDate, " for the purchase of ",
         /Invoice/bookorder/item/quantity, " QTY of book titled ",
         /Invoice/bookorder/item/title, ".")
       </Transform>
    <Transform Algorithm="http://www.w3.org/TR/1999/WD-xml-c14n-19991115"/>
   </Transforms>
   <DigestMethod Algorithm="http://www.w3.org/2000/01/xmldsig/sha1"/>
   <DigestValue Encoding="http://www.w3.org/2000/01/xmldsig/base64">
    KnkofqqssCINlew59DrhE6Hnrpk=
   </DigestValue>
  </Reference>
 </SignedInfo>
 <SignatureValue>
  MCwCFBvOeJygByRVVHjM0YJ47qfkoDITAhRr6u90oIGcXrKz0uNIRJiQTYGRhw==
 </SignatureValue>
 <KeyInfo>
  <X509Data>
   <X509Name>CN=Hiroshi Maruyama, OU=TRL, O=IBM, C=JP</X509Name>
   <X509Certificate>
MIICvTCCAnsCBDhZhc4wCwYHKoZIzjgEAwUAMEQxCzAJBgNVBAYTAkpQMQwwCgYDVQQKEwNJQk
0xDDAKBgNVBAsTA1RSTDEZMBcGA1UEAxMQSGlyb3NoaSBNYXJ1eWFtYTAeFw05OTEyMTcwMDM3
MzRaFw0wMDAzMTYwMDM3MzRaMEQxCzAJBgNVBAYTAkpQMQwwCgYDVQQKEwNJQk0xDDAKBgN
VBAsTA1RSTDEZMBcGA1UEAxMQSGlyb3NoaSBNYXJ1eWFtYTCCAbgwggEsBgcqhkjOOAQBMIIBHwK
BgQD9f1OBHXUSKVLfSpwu7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2y5tVbNeBO4A
dNG/yZmC3a5lQpaSfn+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQTWhaRMvZ1864rYdcq
7/IiAxmd0UgBxwlVAJdgUI8VIwvMspK5gqLrhAvwWBz1AoGBAPfhoIXWmz3ey7yrXDa4V7l5lK+7+jrqgvlXT
As9B4JnUVlXjrrUWU/mcQcQgYC0SRZxl+hMKBYTt88JMozIpuE8FnqLVHyNKOCjrh4rs6Z1kW6jfwv6ITVi
8ftiegEkO8yk8b6oUZCJqIPf4VrlnwaSi2ZegHtVJWQBTDv+z0kqA4GFAAKBgQCE12KsJ2zPP0F+VuR4xGl
Q23ogU47HmOY4TEGrUCuYE9xjqo+Oh/7PtnKj/9+OmSNH1HDiY4GYh3KnjfwB7+2BmAwVLB0kkYZwdc
zb5aok7pj7UQIiRgOp2b/08Fq4ZBDA483SrVwiCvuT3STGQykEyPw4wkXgjpwGb+NDfKUqCzALBgcqhkjO
OAQDBQADLwAwLAIUZeGr8xv9/LwgNBFbr9IkSq2wy5QCFHJOnTNGgisZOI61+O2ycivp0XHE
   </X509Certificate>
  </X509Data>
 </KeyInfo>
</Signature>
```

【書類名】　　要約書

【要約】

【課題】　携帯端末のように計算資源の限られた情報処理端末を用いてＸＭＬ電子署名を行う。

【解決手段】　署名要求者が署名対象文書を生成し（Ｓ１０）、エージェントがこれを受け取る（Ｓ１１）。エージェントによって署名対象文書のサマリテキストが生成され（Ｓ１２）、署名者に送付され、署名者は自己の所有する情報端末でサマリテキストを表示する（Ｓ１３）。その内容を確認（Ｓ１４）の後、署名者はサマリテキストに対して、自己の端末に記録された私有鍵を用いて暗号化し署名をする（Ｓ１５）。署名値はエージェントに送られ（Ｓ１６）、エージェントは署名値を含んだ署名対象文書に対する署名文書を生成する（Ｓ１７）。書名要求者は送付された署名文書を署名者の公開鍵を用いて解読し内容を確認する（Ｓ１７）。

【選択図】　図２

認定・付加情報

特許出願の番号	特願２０００－２６２９５５
受付番号	５０００１１１０３７４
書類名	特許願
担当官	濱谷　よし子　　１６１４
作成日	平成１２年１０月１３日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】　390009531

【住所又は居所】　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】　100086243

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名又は名称】　坂口　博

【代理人】

【識別番号】　100091568

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名又は名称】　市位　嘉宏

【代理人】

【識別番号】　100106699

【住所又は居所】　神奈川県大和市下鶴間１６２３番１４　日本アイ・ビー・エム株式会社大和事業所内

【氏名又は名称】　渡部　弘道

【復代理人】　申請人

【識別番号】　100112520

【住所又は居所】　神奈川県大和市中央林間３丁目４番４号　サクライビル４階　間山・林合同技術特許事務所

【氏名又は名称】　林　茂則

【選任した復代理人】

【識別番号】　100110607

次頁有

認定・付加情報（続き）

【住所又は居所】　神奈川県大和市中央林間３丁目４番４号　サクライビル４階　間山・林合同技術特許事務所
【氏名又は名称】　間山　進也
【選任した復代理人】
【識別番号】　100098121
【住所又は居所】　神奈川県大和市中央林間３丁目４番４号　サクライビル４階　間山・林合同技術特許事務所
【氏名又は名称】　間山　世津子

次頁無

出　願　人　履　歴　情　報

識別番号　　〔３９０００９５３１〕

１．変更年月日　　２０００年　５月１６日
［変更理由］　名称変更
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレーション